What is claimed is:

1. A key agreement method for secure communication in a multiple access system, the key agreement method comprising the steps of:

(a) a first user encoding a signal from a source by a bit sequence and transmitting the signal;

(b) a second user who is a legitimate counterpart of the first user decoding the transmitted signal and measuring the decoded signal;

(c) the second user adopting only bits having the measured value beyond the threshold value which is predetermined;

(d) the second user informing the first user that the bits adopted are the n-th bits in the transmitted bit sequence, not telling the values of the bits; and

(e) the first and second users taking the adopted bits as a key string, and discarding the remaining bits.

2. The method of claim 1, further comprising the steps of:

(f) selecting a subset of bits from the key string shared by the first and second users and checking errors;

(g) if the error rate obtained in (f) is below a tolerable level, considering the transmission safe, accepting the key string and obtaining a refined key string with amplification such as error correction process; and

(h) discarding the key adopted in the step (e) if the error rate obtained in (f) exceeds the tolerable level, returning to the step (a) and performing (a) through (f) until getting the key string which satisfies the condition (g).

3. The method of claim 1, wherein the signal transmitted in the step (a) is susceptible to noise.

4. The method of claim 1, wherein the second user uses a receiver affected by mutual modulated noise by another transmitter.

5. The method of claim 1, wherein the threshold value of the step (c) is determined by the second user considering at least a transmission rate, a transmission error rate, and a degree of security.

6. The method of claim 4, wherein the threshold value of the step (c) is determined by the second user considering at least a transmission rate, a transmission error rate, and a degree of security.